14

OPPORTUNITIES TO ENHANCE INDONESIAN CYBER SECURITY THROUGH THEATER SECURITY COOPERATION

Michael E. Terry

Lieutenant Colonel, US Army

Date Submitted: 26 OCT 2018

Word Count: 4249 words

A paper submitted to the Faculty of the United States Naval War College Newport, RI in partial satisfaction of the requirements of the Department of Joint Military Operations.

DISTRIBUTION A. Approved for public release: distribution unlimited. The contents of this paper reflect the author's personal views and are not necessarily endorsed by the Naval War College or the Department of the Navy.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*
10/26/2018

2. REPORT TYPE

3. DATES COVERED *(From - To)*

4. TITLE AND SUBTITLE
Opportunities to enhance Indonesian cyber security through theater security cooperation

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
LT COL Michael E. Terry

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval War College - Joint Military Operations Department
686 Cushing Road
Newport, RI 02841

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution Statement A: Approved for public release; Distribution unlimited
Reference DOD Directive 5230.24

13. SUPPLEMENTARY NOTES
A paper submitted to the NWC faculty in partial satisfaction of the requirements of the JMO Department. The contents of this paper reflect my own personal views and are not necessarily endorsed by the NWC or the Dept of Navy.

14. ABSTRACT
The emergence of cyberspace as a global commons presents significant challenges for the Republic of Indonesia (ROI). With widespread cyber threats on the rise, opportunities exist to develop a bilateral partnership between the US Indo-Pacific Command (USINDOPACOM) and the ROI to address these challenges under the auspices of theater security cooperations. Available security cooperation tools include military-to-military engagements through personnel exchanges, combine exercises, joint interagency training, and expanded use of the National Guard State Partnership Program (SPP). Maximizing these efforts could have a long-term, positive impact on the development of the Tentara Nasional Indonesia's...

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			Chairman, JMO Dept
					19b. TELEPHONE NUMBER *(Include area code)*
UNCLASS	UNCLASS	UNCLASS		26	401-841-3556

Contents

Abstract

Opportunities to Enhance Indonesian Cyber Security Through Theater Security Cooperation

The emergence of cyberspace as a global commons presents significant challenges for the Republic of Indonesia (ROI). With widespread cyber threats on the rise, opportunities exist to develop a bilateral partnership between the US Indo-Pacific Command (USINDOPACOM) and the ROI to address these challenges under the auspices of theater security cooperation. Available security cooperation tools include military-to-military engagements through personnel exchanges, combined exercises, joint interagency training, and expanded use of the National Guard State Partnership Program (SPP). Maximizing these efforts could have a long-term, positive impact on the development of the Tentara Nasional Indonesia's (TNI) nascent cyber-defense force and pay dividends in the regional collective security of Southeast Asia.

Introduction

The recent emergence of cyberspace as a global commons presents the Republic of Indonesia (ROI) with persistent cybersecurity & defense challenges. By leveraging military-to-military and military-to-civilian engagements to foster bilateral and multilateral relationships, U.S. Indo-Pacific Command (USINDOPACOM) has numerous opportunities to aid the ROI in strengthening its cyber-defense posture, thereby further expanding cybersecurity for the Asia-Pacific Region.

Security cooperation is a tool that aids geographic combatant commanders (GCC) in achieving national security objectives. Deliberately planned, programmed, and integrated into a combatant commander's theater campaign plan, security cooperation activities help to develop relationships with partner nations that encourage them to act in support of our shared strategic objectives.[1]

Security cooperation activities are categorized under the 2017 National Defense Authorization Act (NDAA) into nine mission areas with associated programs and authorities. These categories are 1) military-to-military contacts, 2) personnel exchanges, 3) combined exercises & training, 4) train & equip/provision of defense articles, 5) defense institution building, 6) operational support, 7) education, 8) international armaments cooperation, and 9) humanitarian assistance & disaster relief.[2]

Of these activities, military-to-military contacts, personnel exchanges, combined exercises, and training are areas where USINDOPACOM can apply effort directly or leverage functional

[1] US Department of Defense, *Joint Publication 3-20: Security Cooperation*, (2017), http://www.dtic.mil/doctrine/new_pubs/jp3_20_20172305.pdf, 19-20.
[2] Ibid., 93.

combatant commands and interagency partners to assist in addressing the persistent cyber threat challenging the ROI.

The Economy, Cybersecurity & Cyber Threat Environment in Indonesia

Indonesia has the largest economy in Southeast Asia with a gross domestic product of approximately one trillion US dollars.[3] In 2015, the Indonesian government launched the 2020 Go Digital Vision campaign to spur the country's digital economy, investing over ten billion US dollars in subsidies for the agriculture and fishing industries to incentivize e-commerce conversion and creating one thousand local tech startup companies. The goal of this campaign is to become the largest digital economy in Southeast Asia by 2020.[4] McKinsey & Company, in its 2016 report titled "Unlocking Indonesia's Digital Opportunity" predicted that this digital economy would contribute approximately $150 billion annually to the national economy by 2025.[5] This projected growth in the digital economic sector presents interesting challenges for the ROI given the state of the current cybersecurity threat in the country.

As of 2015, Indonesia was the world's fourth most populous country and had the sixth most internet users in the world.[6] Regarding social media activities, Indonesia is considered highly connected and active, having the fourth largest Facebook and the fifth largest Twitter user bases globally. When considering the rapid growth of the international e-commerce market, these

[3] US Department of State, *Indonesia Integrated Country Strategy*, (2018), https://www.state.gov/documents/organization/284990.pdf, 2.
[4] Henry K. Adikara, "Unleashing Indonesia's Digital Economy Potential," *Jakarta Post*, August 7, 2017, http://www.thejakartapost.com/academia/2017/08/07/unleashing-indonesias-digital-economy-potential.html.
[5] Kaushik Das et al., *Unlocking Indonesia's Digital Opportunity*, (McKinsey & Company, 2016), https://www.mckinsey.com/~/media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking_Indonesias_digital_opportunity.ashx, 14.
[6] Prashanth Parameswaran, "Indonesia's Cyber Challenge Under Jokowi," *Diplomat*, January 21, 2015, https://thediplomat.com/2015/01/indonesias-cyber-challenge-under-jokowi/.

numbers alone are sufficient to highlight the importance of the information communication technology sector in Indonesia.[7]

Unfortunately, the period of 2013-2014 also marked the emergence of Indonesia as one of the world leaders in cybercrime-related activities.[8] During this timeframe, Indonesia consistently ranked in the top three originators of cyber-attack traffic, with Indonesia and China vying for the top two spots in that category and accounting for half of the total attack traffic from the top ten countries internationally.[9] From 2014 to 2015, Indonesia continued to see a dramatic increase in cybercrime, primarily in the e-commerce sector, with the number of cases growing by 389 percent during this timeframe according to Indonesian President Jokowi.[10]

In early 2016, security software company BitDefender ranked India, Indonesia, China, Vietnam, and Thailand as the top five cyber-security risks in the region.[11] Subsequently, the ROI's Political, Legal and Security Affairs Minister indicated that cyber-attacks had risen 33 percent in 2015 compared to the previous year, with 54.5 percent of the attacks aimed at e-commerce related websites.[12] In 2017, Indonesia had the third highest national email malware rate according to cybersecurity giant Symantec, the ninth highest phishing rate, and ranked in the top 10 countries where mobile malware was most frequently blocked.[13]

[7] Leonardus K. Nugraha and Dinita A. Putri, *Mapping the Cyber Policy Landscape: Indonesia*, (London: Global Partners Digital, 2016), https://www.gp-digital.org/wp-content/uploads/2017/04/mappingcyberpolicy_landscape_indonesia.pdf, 8.
[8] Parameswaran, "Indonesia's Cyber Challenge."
[9] Akamai Technologies, *Second Quarter 2013 State of the Internet Report*, (Cambridge, MA, 2013), https://www.akamai.com/us/en/about/news/press/2013-press/akamai-releases-second-quarter-2013-state-of-the-internet-report.jsp.
[10] Ayomi Amindoni, "Indonesia sees drastic increase in cybercrime: Jokowi," *Jakarta Post*, September 20, 2016, http://www.thejakartapost.com/news/2016/09/20/indonesia-sees-drastic-increase-in-cybercrime-jokowi.html.
[11] "Technology: Asia is Top Target for Cyber Attacks," *Asia Times*, September 2, 2016, http://www.atimes.com/article/technology-asia-is-top-target-for-cyber-attacks/
[12] Prashanth Parameswaran, "Does Indonesia Need a New Cyber Agency?," *Diplomat*, September 21, 2016, https://thediplomat.com/2016/09/does-indonesia-need-a-new-cyber-agency/.
[13] Gillian Cleary et al., *Internet Security Threat Report, Volume 23*, (Mountain View, CA: Symantec, 2018), https://www.symantec.com/security-center/threat-report, 69, 72.

To counter Indonesia's growing cyber challenges, President Joko Widowo established Bandan Siber dan Sandi Negara (BSSN), the Indonesian National Cyber and Encryption Agency, in May of 2017. The new agency's responsibilities include protection, recovery, and mitigation against cyber-attacks.[14] In January 2018, President Widowo appointed Major General Djoko Setiadi as head of the BSSN, entrusting ministerial responsibility for national cybersecurity solutions to a military officer with direct reporting authority to the president.[15]Despite taking this basic initial step to protect the nation from cybercrime, the ROI continues to rank 26th of 187 countries that are "exposed" or widely vulnerable to cyber-attacks based on active port scanning according to the National Exposure Index.[16]

Current Status of Theater Security Cooperation Concerning the Indonesia Cyber Threat

A 2013 report by the Center for Strategic and International Security Studies Chair for Southeast Asia Studies entitled "A U.S.-Indonesia Partnership for 2020: Recommendations for Forging a 21st Century Relationship" made numerous political and security cooperation recommendations necessary to further solidify the US-Indonesian bilateral partnership. Of the recommendations contained therein, the following three most readily apply towards addressing Indonesia's cyber defense needs: 1) boost the scope and frequency of bilateral exercises with Indonesia; 2) increase joint training and assistance on cybersecurity between the two nations in combating cyber threats in order to better support private, public and corporate security; and 3)

[14] "Communication Ministry: BSSN Begins to Operate in September," *Tempo*, July 1, 2017, https://en.tempo.co/read/news/2017/07/01/055888091/Communication-Ministry-BSSN-Begins-to-Operate-in-September.
[15] Joko Susilo, "President Installs Djoko Setiadi as Cybersecurity Agency Chief," *Antara News*, January 3, 2018, https://en.antaranews.com/news/114092/president-installs-djoko-setiadi-as-cybersecurity-agency-chief.
[16] *National Exposure Index: Inferring Internet Security Posture by Country Through Port Scanning*, (Boston, MA: Rapid7 Labs, 2018), https://www.rapid7.com/info/national-exposure-index/, 49.

expand and regularize exchanges of military personnel for placement at each other's institutions to continue to build trust and interoperability between the U.S. and Indonesian Armed Forces.[17]

However, based on recent public statements by the GCC, it does not appear that cyber partnership with Indonesia is an area of priority. In a speech on the US-Indonesia bilateral security partnership delivered to the U.S. Indonesia Society & American Chamber of Commerce at Jakarta in August 2017, then-Commander, USINDOPACOM, Admiral Harry Harris made no reference to Indonesia's cybersecurity challenges and failed to highlight this as an area of future area of cooperation between the two nations.[18] Additionally, Admiral Harris' 2016 command guidance did not emphasize cybersecurity defense priorities and cooperation with partners and allies in this area.[19]

Subsequently, both President Donald Trump and Defense Secretary James Mattis emphasized the need for global cybersecurity partnership. In his 2017 National Security Strategy, President Trump pledged to "strengthen America's capabilities—including in space and cyberspace—and revitalize others that have been neglected…[as] allies and partners magnify our power."[20] In translating this commitment to the defense establishment, Secretary Mattis' National Defense Strategy commits to "strengthen our alliances and partnerships in the Indo-Pacific to a networked security architecture capable of deterring aggression, maintaining stability, and ensuring free

[17] Murray Hiebert, Ted Osius, and Gregory B. Poling, *A U.S.-Indonesia partnership for 2020: recommendations for forging a 21st-century relationship*, (Washington, DC: Center for Strategic and International Studies, 2013), https://www.csis.org/analysis/us-indonesia-partnership-2020, 2-3.

[18] Harry B. Harris Jr., "The United States-Indonesia Bilateral Security Partnership" (speech, U.S. Indonesia Society & American Chamber of Commerce, Jakarta, August 7, 2017), http://www.pacom.mil/Media/Speeches-Testimony/Article/1272444/the-united-states-indonesia-bilateral-security-partnership/.

[19] Harry B. Harris Jr., *United States Pacific Command (USPACOM) Guidance*, (Camp Smith, HI: US Pacific Command, 2016), http://www.pacom.mil/Portals/55/Documents/pdf/guidance_12_august_2016.pdf?ver=2016-08-16-140701-960.

[20] Donald J. Trump, *National Security Strategy of the United States of America*, (Washington, DC: The White House, 2017), https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf, 4.

access to common domains,"[21] as well as "invest in cyber defense, resilience, and the continued integration of cyber capabilities into the full spectrum of military operations."[22] Perhaps this renewed strategic emphasis will result in a renewed focus at USINDOPACOM towards expanding bilateral partner efforts in the cybersecurity arena.

In conducting a cursory analysis of this need for more partnership in the areas cyber-defense and cybersecurity, the last two years of data captured in the National Guard State Partnership Program's (SPP) Annual Report to Congress was leveraged. The SPP is a Joint DoD security cooperation program managed by the National Guard Bureau and executed through the GCCs. SPP supports security cooperation efforts within the GCC's area of responsibility (AOR) by connecting the capabilities of the National Guard partner states with a specific country of focus.[23] Data from the 2016 Annual Report reveals that out of eleven total security cooperation engagements with the ROI, none involved cyber-related topics, issues, or training. There were just four cyber-related security cooperation engagements in the entire USINDOPACOM AOR (three in Thailand and one in Tonga) compared to twenty-four total cyber-related exchanges in the US European Command (USEUCOM) AOR in 2016.[24] The 2017 SPP data paints a slightly better picture. Out of twenty total security cooperation engagements with the ROI that year,[25] there was one cyber-related engagement.[26] In the entire USINDOPACOM AOR, there were

[21] James Mattis, *Summary of the 2018 National Defense Strategy of the United States of America*, (Washington, DC: US Department of Defense, 2018), https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, 9.

[22] Ibid., 6.

[23] National Guard Bureau, "State Partnership Program 201 Brief" (presentation, September 1, 2017), https://gko.portal.ng.mil/joint/j5/NGB-J53/NG-J53-SC/PublishingImages/SitePages/Home/SPP%20201%201%20Sept%202017.pptx, 2.

[24] National Guard Bureau, *State Partnership Program FY 2016 Report to Congress*, (Arlington, VA, 2017), https://gko.portal.ng.mil/joint/j5/NGB-J53/NG-J53-SC/SiteAssets/SitePages/Home/FY16%20SPP%20Annual%20Report.pdf, 7, 25-45, 51-52, 54-56.

[25] National Guard Bureau, *State Partnership Program FY 2017 Report to Congress*, (Arlington, VA, 2018), Received via email from the NGB J53 International Affairs Office on September 24, 2018, 7.

[26] Ibid., 58.

thirteen SPP cyber-related engagements (one in Indonesia, six in the Philippines, four in Thailand, and one each respectively in Tonga and Vietnam)[27] but this still lagged behind the 26 events in USEUCOM.[28] It is interesting to note, that of the six cyber engagements conducted by the Hawaii National Guard (HING), the ROI's state partner in the USINDOPACOM AOR, four were conducted with the Philippines while only one was conducted with Indonesia. This indicates that, while the HING is capable of conducting cybersecurity engagements, a disproportional emphasis is being given to other Southeast Asian nations over the ROI.

In an attempt to cast a wider net to see what other DoD agencies are doing to partner with the ROI to aid in combatting their cyber threat, the Global Theater Security Cooperation Management Information System (G-TSCMIS) was leveraged. According to Joint Publication (JP) 3-20, *Security Cooperation*, G-TSCMIS is the authoritative source for DoD security cooperation assessment, planning, execution, monitoring, and evaluation, and serves as the mandatory management repository for all DoD security cooperation data.[29] A review of the G-TSCMIS Military Engagement Theme event report for the fiscal year 2017 indicated that the only cybersecurity cooperation engagement involving the ROI consisted of the five-day subject matter expert exchange (SMEE) conducted by the HING in Jakarta mentioned above. This consisted of a demonstration on cybersecurity focusing on multi-agency coordination and joint operations in support of civil authorities during a cyber-attack or infiltration.[30] Additionally, the 2018 G-TSCMIS indicates only three mil-to-mil engagements involving a cyber-related theme. These included 1) a follow-on SMEE with the HING that built upon the 2017 effort; 2) a two-

[27] Ibid., 58-63.

[28] Ibid., 26-51.

[29] US Department of Defense, "JP 3-20: Security Cooperation," xii.

[30] US Department of Defense, *Global Theater Security Cooperation Management Information System (G-TSCMIS) 2017 Military Engagement Theme Event Report*, (Washington, DC, 2018), accessed October 2, 2018, https://gtscmis.dc3n.navy.mil/, 14-15.

day US Army Pacific (USARPAC) G2-sponsored capabilities presentation and demonstration on intelligence support to cyber defense at Fort Shafter, Hawaii; and 3) a three-day legal SMEE conducted by the USARPAC Staff Judge Advocate (SJA) in Jakarta with TNI lawyers that covered a broad range of topics to include legal issues in cyberspace operations.[31] This indicates that more work lies ahead in leveraging the tools of security cooperation to effectively address the ROIs growing cyber threat environment. It also shows that the National Guard and USARPAC are conducting the bulk of the work in helping the ROI address this threat despite multiple USINDOPACOM commands possessing cyber-defense capabilities or the ability to leverage other DoD assets to assist in addressing this threat. Increasing the impetus for doing more is highlighted by USINDOPACOMs third country objective for the ROI, that "Indonesia builds appropriate defensive cyber capabilities to defend its cyber networks, shares and secures operationally relevant information at the appropriate level of classification, and prevents cyber-attacks from being staged from Indonesia. It has the organizations, personnel, equipment, and management structures to sustain this capacity."[32] This country objective appears to have been added to the GCCs theater strategy during the 2017 timeframe.

Existing Gaps & Opportunities to Strengthen the ROI's Cyber Security Posture

The May 2017 creation of a unifying government agency to address the ROIs persistent cyber threat was a warranted first step. However, many challenges lie ahead for the nation in getting this threat under control. In 2016, leading cybersecurity researchers at Oxford University developed a comprehensive report entitled the "Future of Cybersecurity Capacity in Indonesia."

[31] US Department of Defense, *Global Theater Security Cooperation Management Information System (G-TSCMIS) 2018 Military Engagement Theme Event Report*, (Washington, DC, 2018), accessed October 2, 2018, https://gtscmis.dc3n.navy.mil/, 15-42.

[32] US Department of Defense, *Global Theater Security Cooperation Management Information System (G-TSCMIS) Intermediate Military and Country Objective Assessment Report*, (Washington, DC, 2018), accessed October 2, 2018, https://gtscmis.dc3n.navy.mil/, 25.

Contained therein are twenty recommendations that the ROI can implement to strengthen their national cyber security presence.[33] Of these recommendations, at least three provide USINDOPACOM with opportunity for positive influence through its theater security cooperation by either bringing USINDOPACOM resources to bear or leveraging cross-military or interagency relationships to facilitate capacity building.

The first of these areas involves conducting national-level cyber incident crisis management exercises. The Oxford report recommends that Indonesia's national cybersecurity agency conduct exercises and simulations at the local and national levels at least once a year. And furthermore, these events should involve outside observers to participate in and contribute to the process.[34] This need aligns directly with the JP 3-20 security cooperation category of combined exercises and training, and USINDOPACOM has a long-standing relationship with the TNI through well-established, military-to-military security cooperation exercises.

There are two annual standing exercises that occur between the US and Indonesian Armed Forces. Gema Bhakti is a ten-day joint humanitarian assistance/disaster relief focused exercise that has regularly been occurring since 2014. Typically involving elements from USARPAC, PACFLT, PACAF, HING, and the component forces of the TNI, this exercise focuses on operational-level planning for a response to a natural disaster scenario within the ROI.[35] The USARPAC-sponsored annual exercise, Garuda Shield is primarily an army to army engagement that has been regularly conducted since 2009.[36] Its focus is on exercising combined army capabilities in a stability operations-centric scenario.

[33] Yudhistira Nugraha et al., *The Future of Cyber Security Capacity in Indonesia: Top 20 Recommendations for Strengthening National Cybersecurity Capacity*, (Oxford: University of Oxford Internet Institute, 2016), https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Indonesia%2004-16.pdf, 76-91.

[34] Ibid., 80.

[35] Lenaya Rotklein, "Gema Bhakti Exercise Connects Sailors in Indonesia," United States Pacific Fleet, last modified September 19, 2015, https://www.cpf.navy.mil/news.aspx/030605.

[36] "Exercise Garuda Shield," US Army Pacific, last modified September 18, 2017, https://www.army.mil/standto/2017-09-18.

Based on the FY16-18 data captured in G-TSCMIS, neither of these exercises involves a cyber-defense component in its respective exercise objectives or training strategy. Leveraging the subject matter experience at USINDOPACOM's joint cyber cell, CYBERPAC, the integration of a cyber-defense component in both of these exercises will go a long way towards building an interoperable relationship between the cyber defense forces of the US and Indonesia, enhancing the ROIs ability to protect the global commons of cyberspace within the South Pacific.

A successful model for cyber defense security cooperation through joint exercises is readily evident in USEUCOM. Exercise Baltic Ghost, which is nested under the long-standing Baltic Host exercise series, is a cooperative cyber-defense event with participants from Estonia, Latvia, Lithuania, and their respective National Guard State Partners along with personnel from USEUCOM's joint cyber cell and the NATO Cooperative Cyber Defense Center of Excellence (CCDCoE). Occurring annually since its inception in 2013, this exercise focuses on identifying vulnerable critical infrastructure within the participating host nations, education on the authorities available for collaborative support between military and civil cyber-defense organizations during crisis operations, building public-private cyber partnerships, and effective information sharing operations during peacetime and in the midst of a persistent cyber-attack.[37] A similar exercise model would nest nicely with the Gema Bhakti, as that exercise is largely a headquarters/ministry level operationally focused exercise that tests the exchange of information between institutions in the event of a humanitarian crisis, and practicing the mechanisms for leveraging external support.

[37] "USEUCOM Hosts Cyber Exercise with Baltic Allies," US European Command, last modified July 5, 2017, http://www.eucom.mil/media-library/pressrelease/35877/useucom-hosts-cyber-exercise-with-baltic-allies.

A more tactically-oriented exercise model that would nest consistently with Garuda Shield can be found in Locked Shield. Originally billed as Baltic Cyber Shield, this exercise has occurred annually since 2010 and is a successful model of a multilateral technical defense exercise.[38] Organized as a classic force on force tactical live-fire cyber scenario, a blue team is charged with securing the pre-build IT infrastructure representative of a small company or critical infrastructure service provider while the red team persistently tries to compromise and degrade the system.[39] Technically-oriented exercises of this type are designed to train IT-security students and professionals in network defense techniques, develop best practices in securing critical information infrastructure and supervisory control & data acquisition systems, and increase public-private sector partnership/interagency coordination within the host nation.[40] An exercise following this model would provide a much needed cooperative training forum for the fledgling TNI cyber defense unit, Satuan Siber, which is still very much in its infancy and initial organizational phase, having been established only a year ago.[41] Inviting other network defenders from the governmental sector, such as the Indonesia Security Incident Response Team on Internet Infrastructure/Coordination Center (Id-SIRTII/CC), and the Indonesian Computer Emergency Response Team (ID-CERT) from the public sector will help to foster a robust cooperative cyber defense posture within the region, similar to that in Europe. With time and stable resourcing, the scope of this exercise can be broadened to incorporate other ASEAN

[38] Jaroslaw Jakimczyk, "Largest Cyber-Security Exercise in the World is Being Held in Tallinn," Defence24, last modified April 22, 2016, https://www.defence24.com/largest-cyber-security-exercise-in-the-world-is-being-held-in-tallinn.

[39] *Baltic Cyber Shield Cyber Defence Exercise 2010 After Action Report*, (Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2010), https://ccdcoe.org/multimedia/baltic-cyber-shield-cyber-defence-exercise-2010-after-action-report.html, 3.

[40] Ibid., 4.

[41] Wahyu Purnomo, "TNI Inaugurates Formation of Cyber Unit," *Netral News*, October 14, 2017, http://www.en.netralnews.com/news/currentnews/read/13099/tni.inaugurates.formation.of.cyber.unit

nations to strengthen cooperation to enhance regional security and stability through a multilateral forum.

Assistance to law enforcement through interagency training is another area where USINDOPACOM can help address the ROIs cybersecurity challenges. This activity would be in alignment with the security cooperation pillar of education and the 2013 CSIS recommendation of increasing joint training and assistance on cybersecurity. One of the recommendations from the Oxford study suggests that Indonesian law enforcement capacity needs to be further enhanced to investigate and manage cyber-crime cases, to include developing full investigative measures, digital chain of custody procedures, and management of evidence integrity.[42]

There exists a distinct opportunity here for the GCC to help address this gap by connecting US government (USG) experts in cyber-crime investigations and forensics with Indonesian cyber enforcement professionals through the Joint Interagency Coordination Group (JIACG). Through the JIACG, the GCC can coordinate with the US Department of Justice (DOJ) to export Federal Bureau of Investigation (FBI) trainers to support the ROIs cyber-crime enforcement needs.

The FBI currently offers numerous courses that may help. These include the Advanced Cyber First Responder and Forensics Course, the Online Undercover Operations Training Course, the Use of Analytical Methods in Complex Investigations Course, and the basic through advanced Cyber Crime Investigation Methods Course. Each of these forty-hour courses covers aspects of cyber investigative measures, to include methods to collect and analyze digital evidence, computer/cell phone search and seizure techniques, legal/procedural issues related to using electronic evidence in criminal proceedings, and data recovery from hard drives and removable media. According to G-TSCMIS data, multiple courses have been offered with interpreter

[42] Nugraha, "The Future of Cyber Security Capacity," 87.

support through the USEUCOM JIACG to partner countries, but this capability has not been leveraged in USINDOPACOM.[43] Enhanced training in digital forensics will greatly increase personnel efficiency in investigating cyber-crimes and the likely target audience if coordinated in the ROI would be the Indonesian National Police's Cyber Crime Investigation Center and regional satellite offices.[44]

A third area worth supporting involves further capitalizing on the strengths of the National Guard State Partnership Program by increasing the scope and frequency of cyber-related subject matter expert exchanges. This effort is in line with the security cooperation principle of military-to-military contacts/exchanges and would work towards bridging that gap highlighted in the Oxford study about dedicated military cyber-defense capability in Indonesia. As alluded to earlier, the TNI stood up a military sector cyber-defense unit within the last year.[45] As it is currently in its formative phases, the environment is right to engage TNI leadership and assist in assessing their baseline needs. This assessment could then shape an education, training & equipping strategy that would facilitate the unit's long-term development as a premier cyber defense force, able to serve as a willing and effective collaborative partner in the protection of the digital commons.

Significant cyber defense capacity exists in the National Guard to assist the ROI in addressing their persistent challenges. The four battalions of the Virginia National Guard's 91st Cyber Brigade contain multiple cyber protection teams, cybersecurity companies, and cyber warfare companies.[46] These units conduct defensive cyberspace operations (DCO) which include cyber

[43] US Department of Defense, "G-TSCMIS 2016-2018 Engagement Theme Event Report."

[44] "Indonesian National Police Cyber Crime Directorate Information Brief" (presentation, Cebu, July 2017).

[45] Purnomo, "Formation of Cyber Unit."

[46] National Guard Bureau, "91 Cyber Brigade Unit Page," accessed October 2, 2018, https://gko.portal.ng.mil/states/VA/91/SitePages/Home.aspx.

command readiness inspections, vulnerability assessments, cyber opposing force support (for red team-blue team network defense exercises), critical infrastructure assessments, forensics analysis, theater security cooperation, and train, advise and assist support.[47] In total, the Army National Guard possess over 500 personnel across 23 states dedicated to conducting DCO. Additionally, the Air National Guard possesses four robust cyber operations squadrons, a cyber ISR squadron, and cyber ISR group, spread out across five states that can be leveraged.[48]

Although dedicated cyber defense force structure is absent from the HING (the ROIs State Partner), an initiative is in place that will address this going forward. Recently, National Guard Bureau authorized the states and territories to establish a 12-member ARNG Defensive Cyber Operation Elements (DCOE) to defend the National Guard network, and HING has established these positions under their G6/Information Management Directorate.[49] While predominantly internally focused, the mission scope of the DCOE has recently been expanded for three pilot states (to include Hawaii) to that of a Cyber Mission Assurance Team (CMAT).[50] CMATs are authorized to support domestic interagency/commercial as well as state-partner nations if supporting personnel are converted to Title 10 status. The CMATs work to assure DoD missions through defensive cyber and cyber support activities both on and off the network by conducting risk analysis, vulnerability assessments, threat detection, information sharing, and attack forensics.[51] Moving forward, the HING can leverage its CMAT to expand cyber partnership with Indonesia.

[47] US Army Force Management Support Agency, "Force Management System Web Site," accessed October 2, 2018, https://fmsweb.fms.army.mil/protected/secure/tools.asp.

[48] Jon Soucy, *National Guard Set to Activate Additional Cyber Units,* (National Guard Bureau, 2015), https://www.army.mil/article/159759/National_Guard_set_to_activate_additional_cyber_units/.

[49] US Army Force Management Support Agency, "Force Management System Web Site."

[50] Joseph L. Lengyel, *National Guard Cyber Mission Assurance Team Pilot State Selection,* (Arlington, VA: National Guard Bureau, 2018), received via email from NHARNG G6 on September 21, 2018.

[51] Kelly Hughes, *Position Paper on the Establishment of Cyber Civil Support Teams,* (National Guard Bureau, 2017), received via email from NHARNG G6 on September 21, 2018.

The annual dialogue, or key leader engagement, that occurs between senior leadership of the HING, the ROIs Ministry of Defense and security cooperation planners from USINDOPACOM is the initial touch point to broach the subject of cybersecurity cooperation. Typically scoped to cover all areas of security cooperation assistance available through the SPP, a breakout session can be nested under this engagement to reach consensus on what the TNI sees as their most challenging areas for securing cyberspace. This can be coupled with familiarization visits in which both delegations can see first-hand what each other's respective cyber programs have to offer. Subsequently, the HING can leverage internal subject matter expertise from their DCOE/CMAT and/or partner with personnel from another experienced state to conduct an initial cyber capabilities assessment in order to baseline capabilities and develop a three to five-year engagement plan for the TNI's cyber force. G-TSCMIS data shows that both North Dakota and Utah have recently conducted cyber capability assessments on behalf of their partner nations in other theaters. Additionally, Colorado, Minnesota, and Washington established multi-year cyber engagement strategies for their respective partners in both the EUCOM and INDOPACOM AORs.[52] The lessons learned and methodologies used by each will give some valuable insight to HING planners on how to conduct such an endeavor on behalf of the TNI effectively.

As the HING continues to develop its cyber force structure, it can deliberately partner with other National Guard states that have more routinely provided CDO support to their respective partner nations. For example, the Nebraska and Texas National Guards collaborated on a series of subject matter expert exchanges with the Czech Republic in the EUCOM AOR in 2016 and 2017 that covered a wide array of topics to include cyber contingency planning, network defense, security auditing, information technology certification and accreditation, and biometric program

[52] Extracted from information presented in the NGB's SPP 2016 and 2017 annual reports to Congress as well as information presented in G-TSCMIS Military Engagement Theme Reports for FY 16-18.

development.[53] Collectively sharing best practices, lessons learned and TTPs for conducting military cyber operations creates a mutually-beneficial environment that pays great dividends in solidifying bilateral partnerships.

Counterarguments

There is some debate as to whether greater security cooperation with partner nations is warranted. Obviously, with greater coordination and information exchange concerning cyber vulnerabilities and vulnerability mitigation TTPs there lies an inherent risk that one may reveal intelligence, processes, or mindsets that could benefit adversarial nations.[54] This is especially the case if the information system used to archive records of proceedings, coordination notes, and technical material exchanged has already been breached by an adversarial nation or actor. A delicate balance between information sharing and information security must be struck to maintain a forthcoming and mutually-beneficial open dialogue. Otherwise, trust issues in the bilateral relationship could ensue that could permeate other aspects of the diplomatic relationship.

Another concern with deepening the cybersecurity partnership between the US and the ROI stems from Indonesia's enforcement of cybercrime. The 2008 Indonesian Electronic Information and Transactions (EIT) Law categorizes money laundering, digital pornography, online gambling, and other undesirable internet-based activity as cybercrimes. Additionally, under the provisions of articles 27 and 28, defamation and blasphemy are construed as cybercrimes, carrying stiff penalties of up to six years of imprisonment and/or fines not to exceed one billion

[53] Ibid.

[54] David Inserra, *Cooperation with China and Russia Is Not the Solution for Cyber Aggression*, (Washington, DC: Heritage Foundation, 2017), http://report.heritage.org/ib4748, 2.

rupiah.[55] This is in stark contrast to a constitution that guarantees citizens the freedom of religion and expression in accordance with one's conscience.[56]

The paradox is illuminated when one examines the ROIs track record with enforcing the law. According to the Southeast Asia Freedom of Expression Network, the EIT law is used to suppress freedom of speech, resulting in over 200 internet users being reported to law enforcement for online defamation and blasphemy, many of which were arrested for legitimately expressing their opinion against allegedly corrupt government officials rather than conducting actual defamation.[57] The relative ease with which an offended party can bring criminal charges upon another party in Indonesia, the broad interpretation of the EIT law by the courts when handing down convictions, and the stiff penalties under the law create a potential legitimacy dilemma for the United States. The fundamental question is whether or not it is ethical to increase cybersecurity cooperation initiatives that enhance a nation's capability to prosecute cybercrime that is in stark contradiction with foundational rights enjoyed in the United States.

Conversely, if we do not partner with Indonesia in addressing cybersecurity challenges, there are multiple actors in the Asia-Pacific region that the ROI can turn to for support that do not have our security interests in mind. China and North Korea have demonstrated the capability and willingness to use offensive cyber operations to destabilize the region in order to gain more global influence and realize their national objectives. Additionally, transnational criminal organizations have shown their resolve in utilizing cyberspace to aid in funding their nefarious endeavors. Partnering with the ROI in cyber-defense is in our national interest due to the diffuse

[55] Republic of Indonesia, *Law of the Republic of Indonesia Number 11 Concerning Electronic Information and Transactions*, (2008), http://www.bu.edu/bucflp-fig/files/2012/01/Law-No.-11-Concerning-Electronic-Information-and-Transactions.pdf, 24.
[56] Republic of Indonesia, *1945 Constitution of the Republic of Indonesia, as Amended in 2002*, (2002), http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_174556.pdf, 14.
[57] Arafatul Islam, "Indonesia's Internet Law 'Limits Freedom of Expression'," *Deutsche Welle*, September 22, 2016, https://www.dw.com/en/indonesias-internet-law-limits-freedom-of-expression/a-19568549.

nature of cyber-threats, the pressing need for early attack warning, and the desire for insight into adversarial TTPs to heighten our defensive posture.

Conclusion

The 2018 Department of Defense Cyber Strategy says that the DoD "will work with US allies and partners to strengthen cyber capacity, expand combined cyberspace operations, and increase bi-directional information sharing in order to advance our mutual interests."[58] To date, USINDOPACOM security cooperation activities along this axis have been relatively limited. Examples and lessons learned in other in other theaters such as EUCOM show that endeavors of this nature are warranted, welcomed and effective. The tools of theater security cooperation can provide an avenue for the USINDOPACOM GCC to aid the Republic of Indonesia in addressing their ever-pressing cybersecurity challenges. Enhancing our bilateral partnership through expanding the scope of exercises, leveraging the training capabilities of the interagency, and maximizing the use of the National Guard State Partnership Program will pay great dividends in empowering this partner in Southeast Asia to aid in securing the global commons of cyberspace, a daunting endeavor that cannot be accomplished unilaterally.

[58] US Department of Defense, *Summary of the 2018 Department of Defense Cyber Strategy*, (Washington, DC, 2018), https://gko.portal.ng.mil/arng/G3/ARNGCY/RC%20Cyber%20Updates%20And%20Read%20Aheads/2018%20Cyber-Strategy-Report-Final.pdf, 2.

Bibliography

Adikara, Henry K. "Unleashing Indonesia's Digital Economy Potential." *Jakarta Post*, August 7, 2017. http://www.thejakartapost.com/academia/2017/08/07/unleashing-indonesias-digital-economy-potential.html.

Akamai Technologies. *Second Quarter 2013 State of the Internet Report*. Cambridge, MA, 2013. https://www.akamai.com/us/en/about/news/press/2013-press/akamai-releases-second-quarter-2013-state-of-the-internet-report.jsp.

Amindoni, Ayomi. "Indonesia sees drastic increase in cybercrime: Jokowi." *Jakarta Post*, September 20, 2016. http://www.thejakartapost.com/news/2016/09/20/indonesia-sees-drastic-increase-in-cybercrime-jokowi.html.

Asia Times (Hong Kong). "Technology: Asia is Top Target for Cyber Attacks." September 2, 2016. http://www.atimes.com/article/technology-asia-is-top-target-for-cyber-attacks/.

Baltic Cyber Shield Cyber Defence Exercise 2010 After Action Report. Tallinn, Estonia: NATO Cooperative Cyber Defence Centre of Excellence, 2010. https://ccdcoe.org/multimedia/baltic-cyber-shield-cyber-defence-exercise-2010-after-action-report.html.

Cleary, Gillian, Mayee Corpin, Orla Cox, Hon Lau, Benjamin Nahorney, Dick O'Brien, Brigid O'Gorman, et al. *Internet Security Threat Report, Volume 23*. Mountain View, CA: Symantec, 2018. https://www.symantec.com/security-center/threat-report.

Das, Kaushik, Michael Gryseels, Priyanka Sudhir, and Khoon Tee Tan. *Unlocking Indonesia's Digital Opportunity*. McKinsey & Company, 2016. https://www.mckinsey.com/~/media/McKinsey/Locations/Asia/Indonesia/Our%20Insights/Unlocking%20Indonesias%20digital%20opportunity/Unlocking_Indonesias_digital_opportunity.ashx.

"Exercise Garuda Shield." US Army Pacific. Last modified September 18, 2017. https://www.army.mil/standto/2017-09-18.

Harris Jr., Harry B. *United States Pacific Command (USPACOM) Guidance*. Camp Smith, HI: US Pacific Command, 2016. http://www.pacom.mil/Portals/55/Documents/pdf/guidance_12_august_2016.pdf?ver=2016-08-16-140701-960.

Harris Jr., Harry B. "The United States-Indonesia Bilateral Security Partnership." Speech, U.S. Indonesia Society & American Chamber of Commerce, Jakarta, August 7, 2017. http://www.pacom.mil/Media/Speeches-Testimony/Article/1272444/the-united-states-indonesia-bilateral-security-partnership/

Hiebert, Murray, Ted Osius, and Gregory B. Poling. *A U.S.-Indonesia partnership for 2020: recommendations for forging a 21st century relationship*. Washington, DC: Center for Strategic and International Studies, 2013. https://www.csis.org/analysis/us-indonesia-partnership-2020.

Hughes, Kelly. *Position Paper on the Establishment of Cyber Civil Support Teams*. National Guard Bureau, 2017.
received via email from NHARNG G6 on September 21, 2018

"Indonesian National Police Cyber Crime Directorate Information Brief." Presentation, Cebu, July 2017.
https://rm.coe.int/03-a-country-report-indonesia1/168072bd1f

Inserra, David. *Cooperation with China and Russia Is Not the Solution for Cyber Aggression*. Washington, DC: Heritage Foundation, 2017. http://report.heritage.org/ib4748.

Islam, Arafatul. "Indonesia's Internet Law 'Limits Freedom of Expression'." *Deutsche Welle* (Bonn), September 22, 2016. https://www.dw.com/en/indonesias-internet-law-limits-freedom-of-expression/a-19568549.

Jakimczyk, Jaroslaw. "Largest Cyber-Security Exercise in the World is Being Held in Tallinn." Defence24. Last modified April 22, 2016. https://www.defence24.com/largest-cyber-security-exercise-in-the-world-is-being-held-in-tallinn.

Lengyel, Joseph L. *National Guard Cyber Mission Assurance Team Pilot State Selection*. Arlington, VA: National Guard Bureau, 2018.
Received via email on September 21, 2018 from NHARNG G6.

Mattis, James. *Summary of the 2018 National Defense Strategy of the United States of America*. Washington, DC: US Department of Defense, 2018.
https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.

National Exposure Index: Inferring Internet Security Posture by Country Through Port Scanning. Boston, MA: Rapid7 Labs, 2018. https://www.rapid7.com/info/national-exposure-index/.

National Guard Bureau. *State Partnership Program FY 2016 Report to Congress*. Arlington, VA, 2017. https://gko.portal.ng.mil/joint/j5/NGB-J53/NG-J53-SC/SiteAssets/SitePages/Home/FY16%20SPP%20Annual%20Report.pdf.

National Guard Bureau. *State Partnership Program FY 2017 Report to Congress*. Arlington, VA, 2018.
Received via email on September 24, 2018 from the NGB J53 International Affairs Office.

National Guard Bureau. "State Partnership Program 201 Brief." Presentation, September 1, 2017. https://gko.portal.ng.mil/joint/j5/NGB-J53/NG-J53-SC/PublishingImages/SitePages/Home/SPP%20201%201%20Sept%202017.pptx

National Guard Bureau. "91 Cyber Brigade Unit Page." Accessed October 2, 2018. https://gko.portal.ng.mil/states/VA/91/SitePages/Home.aspx.

Nugraha, Leonardus K., and Dinita A. Putri. "Mapping the Cyber Policy Landscape: Indonesia." Global Partners Digital | Global Partners Digital. Last modified 2016. https://www.gp-digital.org/wp-content/uploads/2017/04/mappingcyberpolicy_landscape_indonesia.pdf.

Nugraha, Yudhistira, Taylor Roberts, Ian Brown, and Ashwin S. Sastrosubroto. *The Future of Cyber Security Capacity in Indonesia: Top 20 Recommendations for Strengthening National Cybersecurity Capacity*. Oxford: University of Oxford Internet Institute, 2016. https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/Indonesia%2004-16.pdf.

Parameswaran, Prashanth. "Does Indonesia Need a New Cyber Agency?" *Diplomat* (Washington DC), September 21, 2016. https://thediplomat.com/2016/09/does-indonesia-need-a-new-cyber-agency/.

Parameswaran, Prashanth. "Indonesia's Cyber Challenge Under Jokowi." *Diplomat* (Washington DC), January 21, 2015. https://thediplomat.com/2015/01/indonesias-cyber-challenge-under-jokowi/.

Purnomo, Wahyu. "TNI Inaugurates Formation of Cyber Unit." *Netral News* (Jakarta), October 14, 2017. http://www.en.netralnews.com/news/currentnews/read/13099/tni.inaugurates.formation.of.cyber.unit.

Republic of Indonesia. *Law of the Republic of Indonesia Number 11 Concerning Electronic Information and Transactions*. 2008. http://www.bu.edu/bucflp-fig/files/2012/01/Law-No.-11-Concerning-Electronic-Information-and-Transactions.pdf.

Republic of Indonesia. *The 1945 Constitution of the Republic of Indonesia, as Amended in 2002*. 2002. http://www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---ilo_aids/documents/legaldocument/wcms_174556.pdf.

Rotklein, Lenaya. "Gema Bhakti Exercise Connects Sailors in Indonesia." United States Pacific Fleet. Last modified September 19, 2015. https://www.cpf.navy.mil/news.aspx/030605.

Soucy, Jon. *National Guard Set to Activate Additional Cyber Units*. National Guard Bureau, 2015. https://www.army.mil/article/159759/National_Guard_set_to_activate_additional_cyber_units/.

Susilo, Joko. "President Installs Djoko Setiadi as Cybersecurity Agency Chief." *Antara News* (Jakarta), January 3, 2018. https://en.antaranews.com/news/114092/president-installs-djoko-setiadi-as-cybersecurity-agency-chief.

Tempo (Jakarta). "Communication Ministry: BSSN Begins to Operate in September." July 1, 2017. https://en.tempo.co/read/news/2017/07/01/055888091/Communication-Ministry-BSSN-Begins-to-Operate-in-September.

Trump, Donald J. *National Security Strategy of the United States of America*. Washington, DC: The White House, 2017. https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905-2.pdf.

US Army Force Management Support Agency. "Force Management System Web Site." Accessed October 2, 2018. https://fmsweb.fms.army.mil/protected/secure/tools.asp.

US Department of Defense. *Joint Publication 3-08: Interorganizational Cooperation*. 2017. http://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_08pa.pdf?ver=2018-02-08-091414-467.

US Department of Defense. *Joint Publication 3-20: Security Cooperation*. 2017. http://www.dtic.mil/doctrine/new_pubs/jp3_20_20172305.pdf.

US Department of Defense. *Summary of the 2018 Department of Defense Cyber Strategy*. Washington, DC, 2018. https://gko.portal.ng.mil/arng/G3/ARNGCY/RC%20Cyber%20Updates%20And%20Read%20Aheads/2018%20Cyber-Strategy-Report-Final.pdf.

US Department of Defense. *Global Theater Security Cooperation Management Information System (G-TSCMIS) Intermediate Military and Country Objective Assessment Report*. Washington, DC, 2018. Accessed October 2, 2018. https://gtscmis.dc3n.navy.mil/.

US Department of Defense. *Global Theater Security Cooperation Management Information System (G-TSCMIS) Military Engagement Theme Event Report*. Washington, DC, 2018. Accessed October 2, 2018. https://gtscmis.dc3n.navy.mil/.

US Department of State. *Indonesia Integrated Country Strategy*. 2018. https://www.state.gov/documents/organization/284990.pdf.

"USEUCOM Hosts Cyber Exercise with Baltic Allies." US European Command. Last modified July 5, 2017. http://www.eucom.mil/media-library/pressrelease/35877/useucom-hosts-cyber-exercise-with-baltic-allies.